UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/719,193	12/08/2000	Louis Goubin	T2146-906738	5716

181 7590 09/07/2005

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/719,193	GOUBIN ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/14/2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *27-47* is/are pending in the application.

4a) Of the above claim(s) *1-26* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *27 and 33* is/are rejected.

7)☒ Claim(s) *28-32 and 34-47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments/Arguments

Claims 1-26 have been cancelled. Applicant's arguments/amendments with respect to amended claims 27-44, previously presented claim 45, and new claims 46-47 filed March 14, 2005 have been fully considered but are moot in view of the new ground(s) of rejection. The Examiner would like to point out that this action is made final since the double patenting rejection was necessitated by the amendments (See MPEP 706.07a).

Double Patenting

I. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

II. Claim 27 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 37 of U.S. Patent No. 6,658,569 (herein after '569 patent). Although the conflicting claims are not identical, they are not patentably distinct from each other because both the present application and the '569 patent relate to process for protecting a computer system against attacks by physical analysis.

Independent claim 1 of the '569 patent includes the steps, as claimed in claim 1 of the present application, of "a) separating the standard cryptographic calculation process into a plurality of distinct calculation process parts; b) executing the distinct calculation process parts in parallel to produce partial intermediate variables distinct from any intermediate variables produced using the standard cryptographic calculation; and c) reconstructing a final value that is identical to the standard final value obtained by the standard cryptographic calculation without separation from said distinct partial intermediate variables whereby the computer system is protected against attacks by physical analysis." Not explicitly disclosed in claim 1 of the '569 patent is applying nonlinear transformations to each of the plurality of partial intermediate variables to create a plurality of partial results. However, claim 37 of the '569 patent includes the step for using "nonlinear transformations of m bits to n bits described by conversion tables" ... "each nonlinear transformation applied to an intermediate variable of the standard cryptographic calculation process," etc. Therefore, independent claim 1 of the application is not patentably distinct from the combination of claims 1 and 37 of the '569 patent and is an obvious embodiment of the '569 patent.

III. Claim 33 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 43 of U.S. Patent No. 6,658,569 (herein after '569 patent). Although the conflicting claims are not identical, they are not patentably distinct from each other because both the present application and the '569 patent relate to process for protecting a computer system against attacks by physical analysis.

Independent claim 1 of the '569 patent includes the steps, as claimed in claim 33 of the present application, of "a) separating the standard cryptographic calculation process into a

plurality of distinct calculation process parts; b) executing the distinct calculation process parts in parallel to produce partial intermediate variables distinct from any intermediate variables produced using the standard cryptographic calculation; and c) reconstructing a final value that is identical to the standard final value obtained by the standard cryptographic calculation without separation from said distinct partial intermediate variables whereby the computer system is protected against attacks by physical analysis." Not explicitly disclosed in claim 1 of the '569 patent is a standard secret key cryptographic algorithm. However, claim 43 of the '569 patent clearly claims that an algorithm is "selected from the group consisting of the DES, Triple DES, and RSA algorithms." Therefore, since DES is form of secret key cryptographic algorithm, independent claim 33 of the application is not patentably distinct from the combination of claims 1 and 43 of the '569 patent and is an obvious embodiment of the '569 patent.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2133
8/19/2005

NK

CHRISTINE T. TU
Primary Examiner

CHRISTINE T. TU
Primary Examiner